Hastings Communications and Entertainment Law Journal

Volume 4 | Number 4 Article 13

1-1-1982

As Interactive Cable Enters, Does Privacy Go out the Window

Gary Selvin

As Interactive Cable Enters, Does Privacy Go Out the Window?

By GARY SELVIN*

I
Introduction

The growth of interactive cable television will provide Americans with the ability to transact more of their business from their homes than ever before. The small plastic keyboard wired to a central computer will enable the user to view cable television programs, take college courses, participate in community action meetings and respond to opinion polls, talk shows and debates.[1] In addition, subscribers will be able to purchase products seen on television by ordering them through their interactive cable system and charging them to their banking or credit accounts. In the future, the system may interact with department stores, service operations, banks, police and fire departments, schools, civic centers and other elements within society. However, these benefits are not without potential disadvantages.

Interactive cable companies will maintain records of transactions between the companies and subscribers. Therefore, it is probable that a composite file will exist for each subscriber. Charles Ferris, ex-Chairman of the Federal Communications Commission expressed his privacy concerns toward interactive cable.

> [A] computer will have a record of what they [the consumers] buy and how much they spend. It will know whether they pay bills quickly, slowly, or not at all, and it will know where their money comes from. It will know whether they watched the debates, or the football game, or a controversial movie. It will know when they came home the previous night—and probably in what condition, depending on how many alarms they accidentally set off. It will know how many people are in their

* Member, Third Year Class; A.B., Occidental College, 1978.

1. Burnham, *The Twists in Two-Way Cable*, CHANNELS, June-July 1981, at 38-43.

houses and in what rooms. In other words, it will know more about them than anyone should.[2]

This capability raises a legal issue yet to be considered by the courts: the violation of individual rights to privacy when interactive cable records are searched by the government. While the maintenance of data by interactive cable companies poses a threat to personal privacy and may subject unknowing users to unwanted intrusions into their homes, these intrusions may be protected by the Fourth Amendment of the United States Constitution and the First Amendment of the California Constitution. This protection is uncertain, however, because different courts apply different standards in evaluating the legitimacy of citizens' privacy expectations.

The degree of expectation may be forecast by analogizing to existing privacy protection in other areas. The records maintained by banks are similar to the financial data which may be stored by interactive cable companies, and numbers recorded by telephone company pen registers[3] are similar to names which may be kept by interactive cable systems. Inconsistencies in state and federal law in these areas demonstrate the difficulty in predicting the standard to be applied. For example, under federal law, bank customers have no expectation of privacy in banking records, and the government need not obtain a warrant to search them.[4] Further, the bank may consent to government searches of its customers' records. By contrast, California law holds that banking records are personal and may not be examined by law enforcement agencies without a warrant.

The United States Supreme Court, interpreting federal law, permits the government to order the telephone company to place a pen register[5] on a customer's phone lines and to compile a list of all telephone numbers dialed without obtaining a warrant.[6] California law yields the opposite result.[7] The state and local governments may not order placement of pen registers without either a warrant or the consent of the customer.

---

2. *Id.* at 43.

3. A pen register is an instrument placed on a telephone line which records all telephone numbers dialed from that phone. Without this device, local numbers go unrecorded.

4. United States v. Miller, 425 U.S. 435 (1976).

5. See note 3, *supra*.

6. Smith v. Maryland, 442 U.S. 735 (1979).

7. People v. McKunes, 51 Cal. App. 3d 487 (1975).

Federal law grants no expectation of privacy to the consumer for bank records and telephone numbers, based on the Supreme Court's interpretation of the United States Constitution. The California Supreme Court extends an expectation of privacy based on their interpretation of the California Constitution and independent state grounds. If these cases are used to determine the expectation of privacy to be applied in cases involving interactive cable records, federal law will not require warrants to review customer records, and California law will require search warrants.

Section II below summarizes current Federal and California privacy law regarding the reasonable expectations of privacy, protection of bank records from government searches and the use of pen registers to record phone numbers dialed by an individual. Section III suggests how current law may be applied to interactive cable. Section IV offers recommendations for safeguarding the privacy of interactive cable users.

II
Modern Privacy Law Against Searches[8]

A. Reasonable Expectation of Privacy

At the heart of modern privacy law is the concept of a reasonable expectation of privacy. The concept was first recognized in English law in the mid-eighteenth century with the notion that man has the right to be free from interference from the government and government efforts to gather criminal evidence.[9] The right to privacy theory was developed to combat physical governmental intrusions. New technology made physical intrusions unnecessary and enabled the government to bend the rules. Use of electronic devices allowed the government to secure evidence while working within the framework of privacy law, for example.

The landmark decision of *Katz v. United States*[10] marked the shift of privacy law from the physical trespass standard. In *Katz*, a "bug" placed on the outside of a telephone booth taped

8. This note will discuss the criminal law interpretation of privacy. The author recognizes that civil law privacy is also an issue in interactive cable and recognizes the possibility of civil damages for an invasion of this privacy. Civil law privacy is beyond the scope of this note, however.

9. Entick v. Carrington, 6 Geo. III, 19 Howell's State Trials 1030 (1765).

10. 389 U.S. 347 (1967).

Katz's conversations without a physical intrusion. The United States Supreme Court held the search unreasonable and thus violative of the Fourth Amendment because there was a reasonable expectation of privacy. The Fourth Amendment protects people not places. Justice Harlan's concurring opinion, which has since become the standard, suggested this guideline:

1. Did the person exhibit an actual expectation of privacy?
2. Was the expectation one that society is prepared to recognize as reasonable?[11]

Further, the Court stated, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[12] The Court insisted on the search warrant requirement stating "[s]earches conducted outside the judicial process, without prior approval by a judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[13] The rationale for this requirement was the elimination of after-the-fact justification for the search.[14]

Without defining terms, the Court advocated the analysis of justification incorporating social considerations and reasonableness.[15]

B. Protection of Bank Records

The expectation of privacy test has been applied by the courts in determining the protection to be afforded to customer's bank records. The rules regarding the right to privacy established in *Katz* and its progeny[16] eroded the long standing rule from *Boyd v. United States*[17] that it was inherently unrea-

11. *Id.* at 361.

12. *Id.* at 351.

13. *Id.* at 357. Unless the delay in procuring a search warrant would endanger lives (Warden v. Hayden, 387 U.S. 294 (1967)) or result in the destruction of evidence (Ker v. California, 374 U.S. 23 (1963)), there must be a search warrant granted under the detached scrutiny of a neutral magistrate.

14. 389 U.S. at 358; Beck v. Ohio, 379 U.S. 89, 96 (1964).

15. Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection*, 43 N.Y.U.L. REV. 968, 983 (1968), analyzes the import of Katz and provides demonstrations of its application. For an example, a narcotics transaction in a highly secluded area in New York's Central Park may have a high degree of freedom from intrusion, but the expectation of privacy and the social acceptance of such an expectation do not warrant protection of the activity.

16. For an analysis of the demise of *Boyd*, a case prior to *Katz*, see Note, *The Life and Times of* Boyd v. U.S. *(1886-1976)*, 76 MICH. L. REV. 184 (1977).

17. 116 U.S. 616 (1886).

sonable for the government to seize documents from a third party, such as a bank, solely because documents were potentially valuable as evidence against the owner. The change culminated in the decision of *United States v. Miller*.[18]

In *Miller*, the government obtained personal banking records as evidence of the overt act necessary to convict the defendants of conspiracy to defraud the United States of tax revenues by manufacturing and selling distilled spirits.[19] The Court of Appeals held that the government must follow legal process[20] before requesting to inspect bank records.[21] Cooperation from the bank did not equal consent of the individual to this inspection.[22] The United States Supreme Court reversed the decision and held there was no legitimate expectation of privacy in the contents of the original checks and deposit slips since the checks were not confidential communications but were negotiable instruments to be used in commercial transactions.[23] Miller had no knowledge of the bank's delivery of the documents pursuant to the subpoena and had voluntarily conveyed all the documents to the bank. The materials were held to be business records of the bank, not Miller's private papers.[24] Furthermore, the Court narrowed the *Katz* holding by stating "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party [the bank] . . . ."[25] This is true even if the information is revealed to the bank on the assumption it will be used for a limited purpose and the confidence will not be betrayed. Thus, the Court concluded that the expectation of privacy is unjustifiable where a third party is involved regardless of the relationship between the bank, the

18. 425 U.S. 435 (1976).

19. *Id.* at 437-438.

20. 500 F.2d 751, 757 (5th Cir. 1974) (quoting Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 52 (1974)).

21. *Id.* at 758.

22. Miller had no knowledge of the subpoena duces tecum obtained by the government to secure the documents. This was not relevant to the decision rendered by the U.S. Circuit Court of Appeals or the Supreme Court. The bank's absence of notification to the depositor is a "neglect without legal consequences here, however unattractive it may be." *Miller* at 443 n.5. Kelley v. United States, 536 F.2d 897 (9th Cir. 1976) reenforced *Miller*. Governmental compulsion of the bank producing records was not against the individual but against the bank. There is no notice requirement.

23. 425 U.S. at 442.

24. *Id.* at 440.

25. *Id.* at 443.

customer and the government.[26]

California courts have upheld depositors' privacy expectations in their bank records, relying upon the California Constitution and independent state grounds in *Burrows v. Superior Court*.[27] In *Burrows*, the court set forth stricter requirements for government access. The legality of the search must be based on either the consent of the depositor or the involvement of the legal process in a search warrant.[28]

In *Burrows*, the court said, "[a] bank customer's reasonable expectation is that, absent compulsion by the legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes."[29] Because of this expectation of privacy, the court mandated that the government obtain a search warrant to review customers' bank records.

The court added consideration of the importance of the activity in contemporary society to the test of reasonable expectation of privacy. "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[30] Bank customers supply this information to aid the bank in their business relationship, but base the usage on their expectation of privacy.[31]

The requirements of consent to the involvement of the legal process were further developed in *Valley Bank of Nevada v.*

---

26. Even if the banks acted as government agents in maintaining and supplying the information, this is not an intrusion upon depositors' Fourth Amendment rights. *Miller* has been highly criticized by criminal law scholars. *See* W. LAFAVE, SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT 411 (1978), in which the author says "The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*."

27. 13 Cal. 3d 238 (1974).

28. *Id.* at 245. The changes in the aftermath of Proposition 8 remain unknown. The Supreme Court will determine the legality of facets of changes in the exclusionary rule and search and seizure law when cases arise. These changes do not change analysis of the law or application to interactive cable.

29. *Id.* at 243.

30. *Id.* at 247.

31. California has codified the confidentiality of bank records and provided standards for government access in Cal. Gov't Code §§ 7460-7490 (West 1980). These sections provide that without either customer authorized disclosure or compliance with the search warrant particularity, state and local governments and agencies may not request originals or copies of information relating to financial institutions' customers from those institutions.

Superior Court.[32] There, the California Supreme Court held that while information disclosed to a bank in confidence may be discoverable, the bank must first make reasonable efforts to locate the customer and notify him of the discovery proceeding and provide him with a reasonable opportunity to object and seek protective court orders.[33] In citing *Burrows*, the court refined the definition of a reasonable expectation of privacy. Based upon the reasonable expectation that the record will be utilized only for internal banking purposes, the court found there was an implied agreement of non-disclosure.[34] That implied agreement justified the expectation of privacy in bank records.

Thus, federal and California courts, interpreting different constitutions, have supplied different meanings of "reasonable expectation of privacy" concerning search and seizure of bank records. The United States Supreme Court, interpreting the United States Constitution, holds that by relinquishing the records to the bank, the depositor simultaneously releases all expectations of privacy in either the original documents or photocopies thereof. The California Supreme Court, interpreting the California Constitution, upholds the concept that the customer in relinquishing these materials to the bank is anticipating the bank will use the information for internal purposes only. The United States Supreme Court holds that bank records are business records, and therefore are outside the scope of personal protection where a subpoena duces tecum is issued to obtain the information. The California Supreme Court finds that because banking is such an integral element in the daily life of an individual, use of a bank does not constitute consent to a search, and privacy is necessary.

C. Protections Against Pen Registers

Pen registers are a relatively new concept in the question of the right to privacy and freedom from unreasonable searches and seizures. The United States Supreme Court has held that pen registers are not to be measured under the protections ac-

32. 15 Cal. 3d 652 (1975). *Valley Bank* is based on civil discovery. The standard for criminal discovery is higher yet.

33. *Id.* at 658.

34. This rule is generally applied in other jurisdictions. First National Bank in Lenox v. Brown, 181 N.W.2d 178, 183 (Iowa 1970); Milohnich v. First National Bank of Miami Springs, 224 So. 2d 759, 761 (Fla. App. 1969).

corded to interceptions of telephone conversations.[35] In *Smith v. Maryland*,[36] the Supreme Court ruled that use of a pen register is not a search within the meaning of the Fourth Amendment and therefore may be conducted without a search warrant.[37]

The United States Supreme Court applied the theory of the reasonable expectation of privacy and held that the suspect did not have the necessary expectation of privacy in the phone numbers dialed to demand protection from the recording of those numbers.[38] The Court analyzed the pen register in light of the two-pronged test of *Katz* and found:

> 1. The suspect entertained no actual expectation as to the numbers he dialed because telephone subscribers know that in the act of dialing they must convey numerical information to the phone company. He could, however, expect to keep the contents of his conversation private.[39]
>
> 2. Even if Smith entertained an expectation of privacy about the numbers he dialed, this expectation is not one society is prepared to recognize as reasonable.[40] By voluntarily dialing, he assumed the risk the company might reveal the information to the police although the company does not normally record the numbers dialed on local calls.[41]

Justice Blackmun, writing for the plurality, also stated, "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[42]

---

35. United States v. New York Telephone Company, 434 U.S. 159 (1977). The standard to be applied to the interception of wire communication is governed by the Omnibus Crime Act, 18 U.S.C. §§ 2510-2520 (1976). Pen registers do not intercept communications.

36. 442 U.S. 735 (1979).

37. 442 U.S. at 742.

38. *Id.* at 743.

39. *Id.* at 741-743.

40. *Id.* at 743-744.

41. *Id.* at 744-745. Nonetheless, 90 years of case law contradicts Justice Blackmun. *See* 389 U.S. at 349.

42. Yale Kamisar, a constitutional law scholar, commented on *Smith*: "It is beginning to look as if the only way someone living in our society can avoid 'assuming the risk' that various intermediary institutions will reveal information to the police is by engaging in drastic discipline . . . characteristic of life under totalitarian regimes." He cites that the alternatives available are foregoing the use of the phone or having the police record all the numbers he dials, foregoing the postal service or having the police collect the names and addresses of all his correspondents and foregoing the use of banks or providing police with access to an enormous quantity of highly personal data. We are talking about unrestrained access to data. "The sky is the limit, aside from

Interpreting California law, the California Court of Appeal has ruled that a customer has the same expectation of privacy for telephone numbers dialed as he does for banking records.[43] The customer has the same expectation that his records will only be used to compute the bill as the bank customer has to believe that records will only be used in the course of business. The California Court of Appeal rejected the argument that the records of the phone calls belonged to the phone company, stating that it is not the telephone that has an expectation of privacy and that the telephone company's rights are not at issue.[44] The telephone company is a neutral party without significant interest and cannot consent to the search of their customers' records on behalf of the customer without his consent.[45]

The California court also applied the *Burrows* analysis in stressing the importance of the telephone in daily life. "It is equally true that, in this age and place, it is virtually impossible for an individual or a business entity to function in the economic sphere without a telephone and that a record of telephone calls also may provide a virtual biography."[46]

In contrast with federal law, the California view of search and seizure is that individuals are entitled to reasonably high standards of protection from intrusion.[47] California attaches a liberal interpretation to the word reasonable, weighing the place of the activity in daily life against the expectation of privacy. Further, California denies that consent by a third party to examine records may substantiate the legality of the search. A neutral third party cannot assert its consent where its function does not coincide with a significant interest. The language in *Burrows* and *McKunes* underscores this theme by holding the right to consent belongs to the customer in each instance.

---

whatever 'self-discipline' the police or other agency may choose to exercise." J. CHOPER, Y. KAMISAR & L. TRIBE, THE SUPREME COURT: TRENDS AND DEVELOPMENTS 1978-1979 143-145 (1979).

43. People v. McKunes, 51 Cal. App. 3d 487 (1975).

44. *Id.* at 492.

45. *Id.*

46. *Id.*

47. California elevated the right to privacy to a constitutional protection and an inalienable right in 1974. CAL. CONST. art. 1, § 1 states:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy."

The federal standard developed in recent court holdings demonstrates a markedly lower level of protection from search and seizure by law enforcement agencies. Concerning banking and phone numbers, the United States Supreme Court holds that because there is no reasonable expectation of privacy in banking and phone numbers, gathering information from those sources does not constitute a search in the context of the Fourth Amendment. Recent decisions have therefore eroded the chances for future findings of other reasonable expectations of privacy under federal law if the same reasoning is applied hereafter.

III
Application of Existing Law to Interactive Cable Systems

A. Overview

The Supreme Courts of the United States and of California have had no opportunity to answer the question of what privacy protections will be given to subscribers of interactive cable. At the moment, the use of two-way cable is limited, and its capabilities are prospective. However, this should not affect the analysis to be applied by the courts when faced with the issue. This section will analyze what restraints courts may apply to government searches of the data bases of two-way cable systems.

Interactive cable has such diverse capabilities that state and federal courts could conceivably choose to analyze interactive systems by components and apply existing law to aspects of interactive cable which are similar to past fact situations. For example, the electronic transfer of funds by the interactive network can be analyzed under the existing law of privacy in banking records. This approach provides only a partial solution because in reviewing the funds transfer records maintained by an interactive cable system, the government may have access to significantly more records than those from which evidence is sought.[48] Therefore, it is critical that the is-

48. While portions of the interactive cable file may be severable from other parts, the risk that evidence obtained in one part of the file will suggest cause to believe that there is further evidence in the remainder of the file demands that the subscribers' records be analyzed as if they were one indivisible entry.

Applying a different standard of privacy for interactive cable produces inconsistent

sue of privacy expectations and the legality of searches of two-way interactive data bases be considered by the courts with respect to all the information in the data bank.

Interactive cable records will include information from all or some of the possible cable applications. These may be gathered from security systems (including when the parties leave the house), smoke detectors (including where flammables are stored), classes taken (including whether or not the student attended), polls (including responses to community, political and general information), funds transferred (including from what account and to which party) and lists of products and services purchased and from which sources. The courts will have to address the issue of whether the government should have unrestricted access and what the Constitutional safeguards should be.

If all the records maintained by the interactive cable company are treated with the expectation of privacy used by the United States Supreme Court in *Miller* and are viewed as documents within a business transaction voluntarily exposed to a third party, there will be no federal expectation of privacy, and a search could be conducted without a search warrant and without the benefit of an impartial magistrate's review. If this approach were taken, it is likely that law enforcement agencies would be able to review the files upon mere issuance of a subpoena.

A significant portion of the records that will be maintained by the cable company are similar to those maintained by the bank in *Miller*. The cable electronic funds transfer and department store credit accounts are tantamount to bank records. The standard for credit cards should follow the reasoning in *Miller*. The language there clearly suggests that under federal law, credit transactions would not be protected. "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."[49] Credit card transactions involve yet another party, the merchant. This further supports the lack of protection and lack of expectation of privacy.

---

levels of privacy between banking through cable and banking through conventional means. The Court would either need to alter the conventional policy of banking privacy or distinguish the expectation of privacy, and hence privacy accorded, between the two alternative banking methods.

49. 425 U.S. at 443.

Under California law, a different conclusion would follow. California applies and interprets its own constitution and therefore is able to recognize the right to privacy to a greater extent than the federal courts do when interpreting federal law. In 1974, California elevated the right to privacy to a constitutionally protected inalienable right.[50] This judicial ideology would likely result in protection of interactive cable subscribers from warrantless searches and seizures. California's protection of bank customers from law enforcement searches of banking transactions without a warrant and telephone subscribers from telephone company use of pen registers suggests the likelihood that California would protect the privacy of interactive cable subscribers.

B. Consent

A subscriber's consent would arguably negate a claim of a reasonable expectation of privacy in the interactive cable data base. Consent to a search of interactive data records might be implied by the subscriber's voluntary participation in the interactive cable service.[51] There is, however, strong legal basis for rejecting an implied consent or waiver of privacy under these circumstances. Under federal law, *Miller* and *Smith* considered relinquishment of information to a third party sufficient to find consent. On this ground, there was no protection accorded. Under California law, the argument that consent vitiates expectations of privacy has been rejected in *Burrows* and *McKunes*. California recognized the importance of banking telephone information and held it negates consent as being tantamount to adhesion.

Interactive cable does not yet have the equivalent value to be considered critical to functioning in modern times. Within the next decade or two, it is probable that interactive cable will be an integral mode of multi-faceted communication. Thus, given the potential and versatility of cable systems, protections akin to those in banking and telephony should be established early to safeguard against unconsented intrusions into privacy.

In both federal and California courts, consent may be analyzed by contract tenets. If as a precursor to purchasing interactive cable service a customer must consent to relinquishing

50. See note 47, *supra*.

51. See *Miller* and *Smith* discussions, sections I-B and I-C, *supra*.

rights to informational privacy, the contract could be adhesive.[52] The subscriber's option would be consent or refusal of the service. This option is ostensibly non-existent because the bargaining positions are so unequal. Under contract analysis, this could be considered an adhesion contract because the superior bargaining position of the interactive cable company renders contract formation unconscionable. The subscriber is given the option: forego privacy or forego interactive cable.

IV
Alternatives

The courts may not presently be prepared to establish a coherent standard for adjudicating the interactive cable system privacy issue. The use of inconsistent standards could subject subscribers to unanticipated intrusions. There are several alternatives to judicial action. Legislatures could regulate the standard at either the federal or state level, federal agencies could establish provisions for dispersal of information or interactive cable companies could place a section within the franchising agreement regarding the right to privacy.

A. Federal Legislation

Passage of federal legislation codifying the constraints to be placed on law and government officials in securing customer records from cable companies may be the best way to establish a clear, consistent standard for all governmental agencies. Within the legislation, Congress could provide rules not only for governmental entities in law enforcement, but could erect a guideline for courts to follow.

In enacting such laws, Congress could apply either the *Miller/Smith* rationale in providing a reduced level of privacy, or follow the *Burrows/McKunes* California law in granting greater rights to privacy. California's approach is preferred because interactive cable may be so intertwined with every fact of daily life as to form a composite of each of the subscribers. Therefore, the national extension of greater rights to privacy may be necessary to prevent obtrusive governmental conduct. However, whether the federal or California standard is applied, federal legislation would enable customers and companies to

52. CALAMARI & PERILLO, CONTRACTS 336-343 (2nd ed. 1977).

realize, in contemplation of cable contracts, what express rights could be anticipated.

The likelihood of passage of federal legislation appears remote in this era of deregulation. Since the late 1970's, for example, the oil, airline and radio-television industries have been deregulated. This trend makes it more probable that the issue of privacy, if legislated, will be governed by the states.

B. State Legislation

State legislation governing the right to privacy in interactive cable would have some of the same benefits as federal legislation. Such laws would codify the question of when law enforcement/government agencies could search interactive cable records. However, in states such as California, which have constitutionalized the right to privacy, the legislation would necessarily fall within the state constitutional protections.

The weakness of legislation at the state level is in the potential inconsistency of laws among states. Interactive cable will involve banking, shopping, other activities between states and the maintenance of information in states different from the subscribers' residences. Because of this, there is a significant possibility of conflicting laws in different states. Differences between the states would present an undue burden on cable companies. While laws would exist as guidelines, there is a question whether the law in the transmitting state, the subscriber's state or the law in the state in which the information was stored would be the applicable law.[53] For these reasons, state legislation is a less effective method of establishing a concrete set of rules for privacy in interactive cable.

C. Franchising Contracts

Some cities with interactive cable systems have required the companies involved to use franchise agreements which extend privacy protections beyond both federal and California case holdings. In Nashville, Tennessee, Citizens for Privacy in Cable TV mounted a campaign to inform citizens of the benefits and burdens of two-way cable. The report stated that the potential abuses must be "acknowledged and honestly dealt

53. For resolution of this conflict of laws question, *see* RESTATEMENT (SECOND) OF CONFLICTS OF LAWS § 152 (1971).

with."[54] The Nashville citizens believed that more was needed than just cable company warnings to subscribers that their interactions could become a matter of public record. To protect subscribers, the organization wrote proposals to be incorporated into the ordinance for franchising.[55]

The organization reasoned that use of a franchise agreement could produce a clear and highly protective privacy standard. The agreement extends privacy coverage beyond both the state and federal levels. It forbids the cable television company from giving information to any third party without the express written consent of the subscriber. The contract is designed to protect the subscriber from intrusions such as those in *Miller*, which held there was no right to privacy.

There are several apparent shortcomings in the contractual approach to privacy law. Foremost, the franchising agreement does not have a proviso which specifies the standard for law enforcement. The unqualified prohibition against giving information to a third party without consent would undoubtedly not include police and government. Therefore, the court would still have to establish the law, deciding whether a subpoena duces tecum or search warrant would be required.[56]

Thus, while the franchising agreement superficially appears to grant the most privacy protection, it leaves critical questions unanswered. So far, the courts have not confronted privacy issues arising from the Nashville franchising agreement. In the future, such a ruling could be useful to other states in assessing the value of application of a franchising agreement for the protection of subscribers.

---

54. *Electronic Nightmare, supra* note 3, at 31.

55. The proposals were as follows:

a. The Cable Television Company is forbidden to give, sell, or otherwise transfer any information about specific subscribers or specific subscribing households to any third party without the express, written consent of such subscriber. Consent may not be obtained through use of the Cable Television System.

b. The Cable Television Company may give, sell, or transfer general information about its entire pool of subscribers or subscribing households to a third party, provided that the information is reduced to a form that does not enable the third party to trace the information provided to specific subscribers, specific households, neighborhoods, or any geographic area more limited than the entire subscriber pool.

Id.

56. Query whether the release of customer records pursuant to a search would subject the interactive cable company to a suit by the subscriber for a breach of contract.

D. Courts' Reconsideration of Present Standards

With the increase in employment and capabilities of interactive cable, the expectation of privacy may be reconsidered. To date, the Supreme Court of the United States has considered the privacy accorded to banking and pen registers independently. In the future, these, and innumerable other detailed records, will be maintained in a single source. The pervasiveness of permitting the government to examine these records exceeds any prior notions. The data therein will not be one facet of life; it will be a dossier. In recognition of this situation, the Supreme Court may have to reevaluate past law. The reconsideration, if any, will not arrive until interactive cable has developed substantially.

California's passage of a constitutional privacy right better prepares that state for adjudicating privacy rights when interactive cable capacities develop. Therefore, it is probable that in California no reconsideration would be forthcoming or necessary.

V
Conclusion

Under current law, drawing from analogy to pen registers and bank records, the federal law would probably not accord a right to privacy to interactive cable records based on *Smith* and *Miller*. Consequently, government seizure of records could be accomplished without the subscriber's consent through the cooperation of the interactive cable company or the issuance of a subpoena duces tecum for the records.

In California, the law recognizes the right to privacy guaranteed by the California Constitution and supported by case law in *Burrows* and *McKunes*. Therefore, without a search warrant which specified the records to be seized, the government would not have access to interactive cable records.

The most effective manner of establishing a clear, concise standard for interactive cable privacy would be the passage of federal legislation. There is little possibility of such enactment. The courts will be forced to grapple with the issue of privacy in interactive cable, but must be wary of making a decision without realizing the practical and social implications. Without recognizing the possibilities, the U.S. Supreme Court could make available a tidy record of individual habits to gov-

ernmental agencies without the necessity of judicial involvement, leaving California law as a bastion of hope for privacy seekers.